REMARKS

Claims 1-3, 5-24, 26-28, 50-51 and 53-68 are pending in the present application. Claims 22, 26, 65, 67 and 68 have been amended.

The amendments to claims 22, 26, 65, 67 and 68 do not add any new matter and are merely intended to correct antecedent basis and/or to clarify claim language at the request of the Examiner. The amendments do not necessitate an further search and should not be used to justify making final any subsequent Office Action.

Claim Objections

The Office Action objected to claims 67 and 68 for errors in the preambles. Appropriate corrections have been made to each claim.

Claim Rejections – 35 USC § 112, Second paragraph

The Office Action rejected claims 14-21 and 61-64 under 35 U.S.C. §112, second paragraph, for allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants respectfully assert that the written description already expressly recites the corresponding structure, material, or acts for performing the claimed functions of the means-plus-function claims presently presented.

37 CFR 1.75(d)(1) requires only that "the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." See MPEP 2181 IV; see also *B. Braun Medical*, 124 F.3d at 1424, 43 USPQ2d at 1900 (holding that 'pursuant to this provision [35 U.S.C. 112, sixth paragraph], structure disclosed in the specification is 'corresponding' structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim."). Thus, the specification must clearly link or associate particular structure to the function recited in the claim. Applicants respectfully assert that the specification provide this required link or association between structure and function.

Express support for the means-plus-function phrases in claim 14 can be found in at least paragraphs [0032]-[0038]. For example, express support for "means for creating a first private key …," and "means for creating a second private key …" is found in at least paragraphs [0032]-[0033]; express support for "means for storing …" is found in at least paragraph [0034]; express

support for "means for outputting the second private key ..." is found in at least paragraphs [0035]-[0037], [0040] and [0063] (using Shamir's sharing scheme); express support for "means for outputting the first public key and the second public key ..." is found in at least paragraph [0035]; and express support for "means for using the first private key for authentication" is found in at least paragraphs [0038]. Similarly, Applicants assert that sufficient support for claims 15-18 is also found in paragraphs [0032]-[0041].

Similar express support for the means-plus-function phrases in claims 19-21 can be found in at least paragraphs [0031] and [0042]-[0048]. Furthermore, similar express support for the means-plus-function phrases in claims 61-64 can be found in at least [0032]-[0041], and [0063].

Applicants accordingly request that the Examiner withdraw the 35 U.S.C. §112, second paragraph rejections of claims 14-21 and 61-64. If further statements are requested, Applicants request that the Examiner specify which means phrases allegedly lack sufficient support in the specification.

Claim Rejections – 35 USC § 101

The Office Action rejected claims 22-24, 26-28 and 65-68 under 35 U.S.C. §101 because the claims are alleged to be directed to non-statutory subject matter. Applicants have amended independent claims 22, 26 and 65, and assert that such amendments overcome these rejections. Applicant respectfully request that the Examiner withdraw the rejection of claims 22-24, 26-28 and 65-68 under 35 U.S.C. §101.

Claim Rejections – 35 USC § 103

The Office Action rejected claims 1-3, 5-9, 11-14, 16-24, 26-28, 50, 51 and 53-68 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Patent No. 6,009,177 (hereinafter "Sudia"). These rejections are respectfully traversed in their entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining

the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Any differences between the prior art and the claims at issue must be such that they would have been obvious to a person having ordinary skill in the art at the time the invention was made. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 167 L.Ed.2d 705, 75 USLW 4289, 82 U.S.P.Q.2d 1385 (2007).

Applicants respectfully submit that the present claims are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al. with Sudia fails to teach or suggest all of the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 50, 51 and 53-68, and one of ordinary skill in the art would not arrive at the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 50, 51 and 53-68 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management. Arthan et al. teaches a private key and public key pair where the private key is encrypted for delivery using a key encryption key (KEK) and stored in an encrypted state at a source computer, where it is decrypted whenever it is needed for use in the transmission of data. See *Arthan et al.* at col. 2, lines 40-48. The keys are generated by a central system 5 and transmitted by the central system 5 to the source and destination systems. *Id.* at col. 3, lines 38-41.

Arthan et al. explains that in order to facilitate the quick change to a new private key, if the existing private key is compromised, the destination system 2 can be supplied in advance with a spare version of the public key. *Id.* at col. 4, lines 15-20. When the private key needs to be changed in the event of a compromise, the version of the private key corresponding to the spare public key can be put into immediate use in the source system 1 as soon as it is supplied. *Id.* at col. 4, lines 20-23. Arthan et al. goes on to state that, since the public and private keys are generated in pairs, the use of spare public keys means that such pairs will have been pre-generated, but that the private key will "need to be held securely after generation and then called up as required." *Id.* at col. 4, lines 25-32.

Notably, Arthan et al. does not provide any further detail regarding how the private key is held securely and does not provide any suggestion that such a private key is output from the device where it is created while another private key is retained. Indeed, based on the disclosure, Applicants assert that Arthan et al. suggests that the private key is generated by and retained (i.e., held) at the central delivery system 5 until which time as it is needed for use. In addition, Arthan et al. does not appear to provide any disclosure relating to the private key being inaccessible. Instead, the disclosure only discusses the private key be compromised. Finally, Arthan et al. does not appear to provide any disclosure about how the private keys are created or whether there is any relationship between the first and second private keys.

Sudia (U.S. Patent No. 6,009,177) – discloses a cryptographic system and method with a key escrow feature for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents. For example, Sudia describes an embodiment in which the device includes a chip that breaks the private key into several pieces and forms a share packet for each trustee or escrow agent designated by the user. (col. 18, lines 12-26). It appears to Applicants from the disclosure in Sudia, that the purpose of keeping the private key with the trustee or escrow agent in Sudia is to verify that the user device is a trusted device and to provide a signed certificate from the master escrow center to be used for communications between devices (see, e.g., col. 20, lines 26-35), and to allow access to the private key by law enforcement for the ability to intercept and decrypt communication to and from a particular user (see, e.g., col. 30, lines 5-19). Applicants are not able to find disclosure, nor has the Examiner identified any disclosure, in Sudia describing the output of one private key and the retention of another private key at the user device. Instead, the only existing private key for the chip is both transmitted to the plurality of different entities and retained stored on the chip for subsequent use by the user device after it is transmitted to the trustee or escrow agent. (col. 17, lines 62-63).

B. Differences Between Claimed Invention and Prior Art

Claims 1-3, 5-10, 14-18, 22-24, 50 and 53-56

Claim 1 recites in part "creating a second private key **associated with the first private key** and creating a second public key corresponding to the second private key at the mobile user device; **outputting the second private key from the mobile user device while retaining the first private key in the mobile user device**, wherein outputting the second private key

comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible."

As noted above, Arthan et al. merely teaches that the private key associated with the spare public key is pre-generated (by the central system 5) and held securely after being generated. Applicant is unable to find, and the Examiner has failed to identify, any other disclosure in Arthan et al. that such a private key is output from the central system 5 while another key is retained and used by the central system 5. Accordingly, Arthan et al. fails to teach or suggest "outputting the second private key from the mobile user device while retaining the first private key in the mobile user device," as recited in independent claim 1.

The failure to teach or suggest any such features alone renders Arthan et al. deficient as a reference against claim 1. However, Arthan et al. also fails to teach or suggest "creating a second private key associated with the first private key." Instead, Arthan et al. merely appears to teach that a second private key is pre-generated by the central system 5. Just being pre-generated does not suggest that the second private key is "associated" with any other private key.

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Arthan et al. In particular, Sudia does not appear to disclose the creation of a second private key associated with the first private key. Additionally, in Sudia, the only existing private key for the chip is both transmitted to the plurality of different entities and retained in storage on the chip for subsequent use by the user device after it is transmitted to the trustee or escrow agent. Thus, the only private key in Sudia is not output while retaining some other private key in the user device.

Applicants respectfully assert that Arthan et al. and Sudia, when combined, do not teach or suggest at least "creating a second private key **associated with the first private key** and creating a second public key corresponding to the second private key at the mobile user device; **outputting the second private key from the mobile user device while retaining the first private key in the mobile user device**, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible," as recited in independent claim 1 and as similarly

recited in independent claim 14, and these differences between claims 1 and 14 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 1 and 14.

Similarly, Arthan et al. and Sudia, when combined, do not teach or suggest at least "create a second private key **associated with the first private key** and create a second public key corresponding to the second private key; retain the first private key and output the second private key as a plurality of shares to a plurality of different entities once **such that the second private key can be re-created and used when there is no access to the first private key**," as recited in independent claim 22, and these differences between claim 22 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 22.

Finally, Arthan et al. and Sudia, when combined, do not teach or suggest at least " a processor configured to: ... generate a second private key **associated with the first private key**; ... a transmitter coupled to the processor to: output the second private key as a plurality of shares to a plurality of different entities once, **such that the second private key can be re-created and used when there is no access to the first private key**," as recited in independent claim 50, and these differences between claim 50 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 50.

Furthermore, the nonobviousness of independent claims 1, 14, 22 and 50 precludes a rejection of claims 2, 3, 5-10, 15-18, 23, 24 and 53-56, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 2, 3, 5-10, 15-18, 23, 24 and 53-56, in addition to the rejection to independent claims 1, 14, 22 and 50.

Claims 11-13, 19-21, 26-28 and 51

Claim 11 recites, in part, "receiving a second public key from the mobile user device, the second public key **associated with the first public key**, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created and used **when there is no access to a first private key** corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication."

As noted above, Arthan et al. teaches the use of private and public key pairs, and the use of a spare public key. However, Arthan et al. fails to teach that the spare public key is associated with another public key. Instead, Arthan et al. appears to be silent regarding how the key pairs are created.

In addition, Arthan et al. fails to teach that the spare public key has a corresponding private key that can be re-created and used when there is no access to a private key that corresponds with the other public key. In other words, Arthan et al. discloses only that the private key corresponding to the spare public key is used only when the active private key is either expired or compromised. Arthan et al. seems to suggest that a key is compromised when it is known to an unintended device. See, *e.g.*, *Arthan et al.* at col. 3, lines 19-24 (stating that when the private key is compromised, the private key must not be treated as a valid key, which infers that the compromised private key is still accessible since the destination system may still be receiving data signed with the compromised key). Thus, Arthan et al. fails to teach or suggest that the private key corresponding to the spare public key is used when there is no access to a first private key corresponding to a first public key. Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al. and Sudia, when combined, do not teach or suggest at least "receiving a second public key from the mobile user device, the second public key **associated with the first public key**, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created and used **when there is no access to a first private key** corresponding to the first public key," as recited in independent claims 11 and 19, and as similarly recited in

independent claims 26 and 51, and these differences between claims 11, 19, 26 and 51 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 11, 19, 26 and 51.

Furthermore, the nonobviousness of independent claims 11, 19 and 26 precludes a rejection of claims 12, 13, 20, 21, 27 and 28, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 12, 13, 20, 21, 27 and 28, in addition to the rejection to independent claims 11, 19, 26 and 51.

Claims 57-68

New independent claim 57 recites "re-creating a second private key **at a mobile user device that has no access to a first private key associated with the second private key**, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; and using the second private key for authentication of the mobile user device." Independent claims 61 and 65 also include similar recitations.

As noted above, Arthan et al. does not provide any teachings or suggestions that a compromised private key means that the private key is not accessible to a device using the compromised private key. Instead, Arthan et al. appears to suggest that a compromised private key merely refers to a private key that has be cracked or accessed by an unintended party. See, *e.g.*, *Arthan et al.* at col. 3, lines 19-24; and col. 5, lines 30-35. As Arthan et al. fails to provide any such disclosure, Arthan et al. fails to teach or suggest "re-creating a second private key at a mobile user device that has no access to a first private key." In addition, Arthan et al. does not teach or suggest that any of the private keys are associated with other private keys. Therefore, there is no disclosure in Arthan et al. relating to "a first private key associated with the second private key." As a result, Arthan et al. fails to teach or suggest "re-creating a second private key at a mobile user device that has not access to a first private key associated with the second private key," as recited in independent claim 57.

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Arthan et al. with respect to independent claims 57, 61 and 65.

Applicants respectfully assert that Arthan et al. and Sudia, when combined, do not teach or suggest at least "re-creating a second private key **at a mobile user device that has no access to a first private key associated with the second private key**, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; and using the second private key for authentication of the mobile user device," as recited in independent claim 57, and as similarly recited in independent claims 61 and 65, and these differences between claims 57, 61 and 65 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 57, 61 and 65.

Furthermore, the nonobviousness of independent claims 57, 61 and 65 precludes a rejection of claims 58-60, 62-64 and 66-68, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 58-60, 62-64 and 66-68, in addition to the rejection to independent claims 57, 61 and 65.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: November 1, 2010

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502